Electronic Version

Stylesheet Version v1.1.1

Description

METHODS AND APPARATUS FOR A SECURE PROXIMITY INTEGRATED CIRCUIT CARD TRANSACTIONS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This invention claims priority to U.S. Patent Application No. 10/192,488, entitled "SYSTEM AND METHOD FOR RFID PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed on July 9, 2002 (which itself claims priority to U.S. Provisional Patent Application No. 60/277,539, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTION" filed March 20, 2001), and to U.S. Provisional Patent Application No. 60/396,577, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed on July 16, 2002, all of which are incorporated herein by reference.

FIELD OF INVENTION

[0002] The present invention relates generally to the use of integrated circuit cards, or "smartcards," for completing transactions and, more particularly, to methods and apparatus for secure data transfer between a smartcard and a merchant system.

BACKGROUND OF INVENTION

[0003] Companies that provide transaction accounts for purchasing goods and services are constantly looking for ways to increase the number of consumers using the companies" services. One way to encourage consumer use is ensure that consumer's shopping experience is pleasant and convenient. Many efforts for enhancing the convenience of the shopping experience focus on the speed at which the transaction is completed. The faster the transaction is completed, the more pleasant and convenient the shopping experience for the consumer. This need for speed has resulted in the development of payment devices designed to replace conventional credit cards and checks, the use of which results in a transaction dependent upon the alacrity of the persons involved in the transaction. For example, conventional credit cards and checks often must be temporarily relinquished, for example, to a cashier for transaction completion, and the transaction is completed only as quickly as the cashier moves.

[0004] The more recently developed payment devices do not have to be relinquished since the payment devices are capable of completing a transaction in a contactless environment. Particularly, the consumer may maintain control of the payment device during completion of the entire transaction since the payment device does not have to be "swiped" or inserted in a card reader to be read (e.g., data stored on the card is retrieved). This is, in turn, removes the need for handing over the payment device to a cashier who ordinarily increases the time for transaction completion.

[0005] One type of payment device that has become popular for use in speeding up a transaction is the integrated circuit card, or "smartcard." The term "smartcard" refers generally to wallet-sized or smaller payment devices incorporating a microprocessor or microcontroller to store and manage data within the card. More complex than magnetic-stripe and stored-value cards, smartcards are characterized by sophisticated memory management and security features. A typical smartcard includes a microcontroller embedded within the card plastic which is electrically connected to an array of external contacts provided on the card exterior. A smartcard microcontroller generally includes an electrically-erasable and programmable read only memory (EEPROM) for storing user data, random access memory (RAM) for scratch storage, and read only memory (ROM) for storing the card operating system. Relatively simple microcontrollers are adequate to control these functions. Thus, it is not unusual for smartcards to utilize 8-bit, 5 MHZ microcontrollers with about 8K of EEPROM memory (for example, the Motorola 6805 or Intel 8051 microcontrollers).

[0006] A number of standards have been developed to address general aspects of integrated circuit cards, e.g.: ISO 7816-1, Part 1: Physical characteristics (1987); ISO 7816-2, Part 2: Dimensions and location of the contacts (1988); ISO 7816-3, Part 3: Electronic signals and transmission protocols (1989, Amd. 1 1992, Amd. 2 1994); ISO 7816-4, Part 4: Inter-industry commands for interchange (1995); ISO 7816-5, Part 5: Numbering system and registration procedure for application identifiers (1994, Amd. 1 1995); ISO/IEC DIS 7816-6, Inter-industry data elements (1995); ISO/IEC WD 7816-7, Part 7: Enhanced inter-industry commands (1995); and ISO/IEC WD 7816-8, Part 8: Inter-industry security architecture (1995). These standards are hereby incorporated by reference. Furthermore, general information regarding magnetic stripe cards and chip cards can be found in a number of standard texts, e.g., Zoreda & Oton, "Smart Cards" (1994), and Rankl & Effing, "Smart Card Handbook" (1997), the contents of which are hereby incorporated by reference.

[0007] Another payment device that is becoming more popular for use in speeding up a transaction uses Radio Frequency Identification (RFID) technology for data transfer. Of late, companies are increasingly embodying RFID data acquisition technology in a fob, tag or other similar form factor for use in completing financial transactions. A typical fob includes a transponder and is ordinarily a self-contained device, which may be contained on any portable form factor. In some instances, a battery may be included with the fob to power the transponder, in which case, the internal circuitry of the fob (including the transponder) may draw its operating power from the battery power source. Alternatively, the fob may exist independent of an internal power source. In this instance the internal circuitry of the fob (including the transponder) may gain its operating power directly from a RF interrogation signal. U.S. Patent No. 5,053,774, issued to Schuermann, describes a typical transponder RF interrogation system, which may be found in the prior art. The Schuermann patent describes in general the powering technology surrounding conventional transponder structures. U.S. Patent No. 4,739,328, issued to Koelle, et al., discusses a method by which a conventional transponder may respond to a RF interrogation signal. Other typical modulation techniques, which may be used, include, for example, ISO/IEC 14443 and the like.

[0008] In conventional fob powering technologies, the fob is typically activated upon presenting the fob in an interrogation signal. Alternatively, the fob may have an internal power source such that interrogation by the reader to activate the fob is not required. In either case, the fob does not have to be relinquished to a cashier, thereby speeding up transaction completion.

[0009] One of the more visible uses of the RFID technology is found in the introduction of Exxon/Mobil's Speedpass® and Shell's EasyPay® products. These products use transponders placed in a fob or tag, which enables automatic identification of the user when the fob is presented at a Point of Sale (POS) device. Fob identification data is typically passed to a third-party server database, where the identification data is referenced to a customer (e.g., user) credit or debit account.

[0010] One disadvantage with the conventional uses of the RFID technology is that conventional RFID devices may transmit only a limited amount of information (e.g., the device identifier) to the merchant system for processing. The advantage of transmitting data using Radio Frequency (RF), however, has not gone unnoticed. Some companies, such as American Express, have developed payment devices, which combine the integrated circuitry found in smartcard technology with the transponder powering technology found in conventional RFID devices. U.S. Patent Application No. 10/192,488, filed July 9, 2002, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," incorporated herein by reference (incorporated herein by reference), teaches such a device.

[0011] Figure 9 illustrates a block diagram of the many functional blocks of an exemplary RF operable payment device fob 902 which is taught in the '488 application. Fob 902 may be a RFID fob 902 which may be presented by the user to facilitate an exchange of funds or points, etc., for receipt of goods or services. As described herein, by way of example, the fob 902 may be a RFID fob, which may be presented for facilitating payment for goods and/or services.

[0012] Fob 902 may include an antenna 903 for receiving an interrogation signal from a RFID reader (not shown) via antenna 903 (or alternatively, via external antenna 918 in communication with a transponder 920). Fob antenna 903 may be in communication with a transponder 914. In one exemplary embodiment, transponder 914 may be a 13.56 MHz transponder compliant with the ISO/IEC 14443 standard, and antenna 903 may be of the 13 MHz variety. The transponder 914 may be in communication with a transponder compatible modulator/demodulator 906 configured to receive the signal from transponder 914 and configured to modulate the signal into a format readable by any later connected circuitry. Further, modulator/demodulator 906 may be configured to format (e.g., demodulate) a signal received from the later connected circuitry in a format compatible with transponder 914 for transmitting to RFID reader via antenna 903. For example, where transponder 914 is of the 13.56 MHz variety, modulator/demodulator 906 may be ISO/IEC 14443-2 compliant.

[0013] Modulator/demodulator 906 may be coupled to a protocol/sequence controller 908 for facilitating control of the authentication of the signal provided by RFID reader, and for facilitating control of the sending of the fob 902 account number. In this regard, protocol/sequence controller 908 may be any suitable digital or logic driven circuitry capable of facilitating determination of the sequence of operation for the fob 902 inner-circuitry. For example, protocol/sequence controller 908 may be configured to determine whether the signal provided by the RFID reader is authenticated, and thereby providing to the RFID reader the account number stored on fob 902.

[0014] Protocol/sequence controller 908 may be further in communication with authentication circuitry 910 for facilitating authentication of the signal provided by RFID reader. Authentication circuitry may be further in communication with a non-volatile secure memory database 912. Secure memory database 912 may be any suitable elementary file system such as that defined by ISO/IEC 7816-4 or any other elementary file system allowing a lookup of data to be interpreted by the application on the chip. The data may be used by protocol/sequence controller 908 for data analysis and used for management and control purposes, as well as security purposes. Authentication circuitry may authenticate the signal provided by RFID reader by association of the RFID signal to authentication keys stored on database 912. Encryption circuitry may use keys stored on database 912 to perform encryption and/or decryption of signals sent to or from the RFID reader.

[0015] In addition, protocol/sequence controller 908 may be in communication with a database 914 for storing at least a fob 902 account data, and a unique fob 902 identification code. Protocol/sequence controller 908 may be configured to retrieve the account number from database 914 as desired. Database 914 may be of the same configuration as database 912 described above. The fob account data and/or unique fob identification code stored on database 914 may be encrypted prior to storage. Thus, where protocol/sequence controller 908 retrieves the account data, and or unique fob identification code from database 914, the account number may be encrypted when being provided to RFID reader. Further, the data stored on database 914 may include, for example, an unencrypted unique fob 902 identification code, a user identification, Track 1 and Track 2 data, as well as specific application applets. In a typical transaction, a consumer may present the fob 902 to a merchant reader (not shown) for transaction completion. The merchant reader may receive information from the fob database 912, 914 to be transferred to the account issuer for transaction completion.

[0016] While use of the smartcard and RF technologies results in a faster and more convenient transaction, the method of data transfer between the payment device and the merchant system must be secured against fraud. As such, a need exists for a method of securing the transaction which does not increase the time needed to complete a transaction, and which method may be used without device user intervention.

SUMMARY OF INVENTION

[0017] The present invention provides methods and apparatus for transaction completion using a proximity integrated circuit payment device. The system includes a "smartcard" that may be operable to transmit data to a merchant system via RF. The smartcard is operable to indicate to the merchant system various transaction authorization methods and to provide authentication data without intervention from the smartcardholder.

[0018] The system of the present invention includes a smartcard in communication with a merchant smartcard or RF reader for communicating cardholder authentication and transaction authorization data. The merchant system is in communication with a transaction account issuer system, and optionally an alternate identification server, for transmitting transaction information and receiving transaction authorization, and for receiving transaction settlement. In a typical method according to the invention, the cardholder may provide a smartcard to a merchant system to permit the merchant system to read the data contained thereon. The merchant system may then select the appropriate processing application by matching the compatible transaction applications on the merchant system with those contained on the smartcard. The merchant system may then retrieve information from the smartcard, determine whether the application should be completed online or offline and whether there are transaction or usage restrictions placed on the transaction account. In determining whether to complete the transaction online or offline, the merchant system takes into consideration various merchant terminal risk factors defined by the merchant. During online transactions, the method contemplates the results of a smartcard risk factor analysis performed by the smartcard.

Brief Description of Drawings

[0019] The present invention will hereinafter be described in conjunction with the appended drawing figures, wherein like numerals denote like elements, and:

[0020] Figure 1 illustrates an exemplary smartcard apparatus;

[0021] Figure 2 is a schematic diagram of an exemplary smartcard integrated circuit, showing various functional blocks;

[0022] Figure 3 is an exemplary diagram of files and directories arranged in a typical tree structure;

[0023] Figure 4 sets forth an exemplary database structure in accordance with a preferred embodiment of the present invention;

[0024] Figure 5 sets forth an exemplary payment system application data structure in accordance with the present invention;

[0025] Figure 6 sets forth a block diagram of a preferred transaction completion system data structure in accordance with the present invention;

[0026] Figure 7 sets forth a flow chart diagramming a transaction method in accordance with the present invention;

[0027] Figure 8 illustrates an exemplary distributed transaction system useful in practicing the present invention;

[0028] Figure 9 illustrates an exemplary RF/RFID payment device useful in practicing the present invention;

[0029] Figure 10 is a block diagram of an exemplary RF/RFID reader useful in practicing the present invention;

[0030] Figure 11 is a flow chart of an exemplary protocol/sequence controller decision process useful with the present invention; and

[0031] Figure 12 depicts and exemplary flow diagram for the operation of a typical RFID payment device in accordance with the present invention.

DETAILED DESCRIPTION

[0032] The present invention may be described herein in terms of functional block components, screen shots, optional selections and various processing steps. Such functional blocks may be realized by any number of hardware and/or software components configured to perform to specified functions. For example, the present invention may employ various integrated circuit components (e.g., memory elements, processing elements, logic elements, look-up tables, and the like), which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language such as C, C++, Java, COBOL, assembler, PERL, extensible markup language (XML), JavaCard and MULTOS with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. For a basic introduction on cryptography, review a text written by Bruce Schneier entitled "Applied Cryptography: Protocols, Algorithms, and Source Code in C," published by John Wiley & Sons (second edition, 1996), herein incorporated by reference.

[0033] In addition, many applications of the present invention could be formulated. The exemplary network disclosed herein may include any system for exchanging data or transacting business, such as the Internet, an intranet, an extranet, WAN, LAN, satellite communications, and/or the like. It is noted that the network may be implemented as other types of networks, such as an interactive television network (ITN).

[0034] Where required, the system user may interact with the system via any input device such as, a keypad, keyboard, mouse, kiosk, personal digital assistant, handheld computer (e.g., Palm Pilot®, Blueberry®), cellular phone, and/or the like. Similarly, the invention could be used in conjunction with any type of personal computer, network computer, work station, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows 2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, Solaris, or the like. Moreover, although the invention may frequently be described as being implemented with TCP/IP communications protocol, it should be understood that the invention could also be implemented using SNA, IPX, Appletalk, IPte, NetBIOS, OSI, or any number of communications protocols. Moreover, the system contemplates, the use, sale, or distribution of any goods, services or information over any network having similar functionality described herein.

[0035] A transaction device identifier, as used herein, may include any identifier for a transaction device, which may be correlated to a user transaction account (e.g., credit, charge debit, checking, savings, reward, loyalty, or the like) maintained by a transaction account provider (e.g., payment authorization center). A typical transaction account identifier (e.g., account number) may be correlated to a credit or debit account, loyalty account, or rewards account maintained and serviced by such entities as American Express, Visa and/or MasterCard, or the like.

[0036] To facilitate understanding, the present invention may be described with respect to a credit account. However, it should be noted that the invention is not so limited and other accounts permitting an exchange of goods and services for an account data value is contemplated to be within the scope of the present invention.

[0037] A transaction device identifier may be, for example, a sixteen-digit credit card number, although each credit provider has its own numbering system, such as the fifteen-digit numbering system used by American Express. Each company's credit card numbers comply with that company's standardized format such that the company using a sixteen-digit format will generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000". In a typical example, the first five to seven digits are reserved for processing purposes and identify the issuing bank, card type and, etc. In this example, the last sixteenth digit is used as a sum check for the sixteen-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer. The account number may be stored as Track 1 and Track 2 data as defined in ISO/IEC 7813, and further may be made unique to the RFID transaction device.

[0038] In one exemplary embodiment, the transaction device identifier may include a unique RFID transaction device serial number and user identification number, as well as specific application applets. The transaction device identifier may be stored on a transaction device database located on the transaction device. The transaction device database may be configured to store multiple account numbers issued to the RFID transaction device user by the same or different account providing institutions. In addition, where the device identifier corresponds to a loyalty or rewards account, the RFID transaction device database may be configured to store the attendant loyalty or rewards points data.

[0039] The databases discussed herein may be any type of database, such as relational, hierarchical, object-oriented, and/or the like. Common database products that may be used to implement the databases include DB2 by IBM (White Plains, New York), any of the database products available from Oracle Corporation (Redwood Shores, California), Microsoft Access or MSSQL by Microsoft Corporation (Redmond, Washington), or any other database product. Database may be organized in any suitable manner, including as data tables or lookup tables. Association of certain data may be accomplished through any data association technique known and practiced in the art. For example, the association may be accomplished either manually or automatically. Automatic association techniques may include, for example, a database search, a database merge, GREP, AGREP, SQL, and/or the like. The association step may be accomplished by a database merge function, for example, using a "key field" in each of the manufacturer and retailer data tables. A "key field" partitions the database according to the high-level class of objects defined by the key field. For example, a certain class may be designated as a key field in both the first data table and the second data table, and the two data tables may then be merged on the basis of the class data in the key field. In this embodiment, the data corresponding to the key field in each of the merged data tables is preferably the same. However, data tables having similar, though not identical, data in the key fields may also be merged by using AGREP, for example.

[0040] In addition to the above, the transaction device identifier may be associated with any secondary form of identification configured to allow the consumer to interact or communicate with a payment system. For example, the transaction device identifier may be associated with, for example, an authorization/access code, personal identification number (PIN), Internet code, digital certificate, biometric data, and/or other secondary identification data used to verify a transaction device user identity.

[0041] It should be further noted that conventional components of RFID transaction devices and smartcards may not be discussed herein for brevity. For example, one skilled in the art will appreciate that the RFID transaction device and the RFID reader disclosed herein include traditional transponders, antennas, protocol sequence controllers, modulators/demodulators and the like, necessary for proper RFID data transmission. As such, those components are contemplated to be included in the scope of the invention.

[0042] It should also be noted that the present invention is described with respect to an integrated circuit card, such as, a smartcard, by way of example and not of limitation. That is, other integrated circuit card devices are contemplated to be within the scope of the invention. For example, the transaction device described with respect to Figure 9 is useful for the present invention. Additionally, although the present invention is described with reference to a "card" the term card is used herein to refer to any integrated circuit transaction device containing an integrated circuit card payment application. That is, the term "card" is not limited by the size or shape of the form factor.

[0043] To facilitate an understanding of the invention, the general operation and structure of a smartcard useful with the invention is discussed. Referring now to Figures 1 and 2, an exemplary smartcard system suitable for practicing the present invention is shown. A smartcard 100 generally comprises a card body 102 having a communication region 104 for providing contact or non-contact communication between an external device (e.g., a card reader) and an integrated circuit 110 encapsulated within card body 102. Communication region 104 preferably comprises six conductive pads 106 whose placement and size conform to ISO7816-2. More particularly, a communication region 104 in conformance with ISO-7816-2 preferably comprises VCC contact 106(a) (power supply), RST contact 106(b) (reset), CLK contact 106(c) (external clock), GND Contact 106(d) (ground), VPP contact 106(e) (programming voltage), and I/O contact 106(f) (data line).

[0044] VCC 106(a) suitably provides power to IC 110 (typically 5.0 V +/- 10%). CLK 106(c) is suitably used to provide an external clock source, which acts as a data transmission reference. RST 106(b) is suitably used to transmit a reset signal to IC 110 during the booting sequence. VPP contact 106(e) may be used for programming of EEPROM 212 in IC 110. As is known in the art, however, this contact is generally not used since modern ICs typically incorporate a charge pump suitable for EEPROM programming which takes its power from the supply voltage (VCC 106(a)). I/O 106(f) suitably provides a line for serial data communication with an external device, and GND 106(d) is suitably used to provide a ground reference. Encapsulated integrated circuit 110 is configured to communicate electrically with contacts 106 via any number of known packaging techniques, including, for example, thermosonically-bonded gold wires, tape automated bonding (TAB), and the like.

[0045] While an exemplary smartcard is discussed above in the context of a plurality of external contacts, it will be appreciated that contactless cards may also be utilized to practice this invention. That is, non-contact communication methods may be employed using such techniques as capacitive coupling, inductive coupling, and the like. As is known in the art, capacitive coupling involves incorporating capacitive plates into the card body such that data transfer with a card reader is provided through symmetric pairs of coupled surfaces, wherein capacitance values are typically 10-50 picofarads, and the working range is typically less than one millimeter. Inductive coupling employs coupling elements, or conductive loops, disposed in a weakly-coupled transformer configuration employing phase, frequency, or amplitude modulation. In this regard, it will be appreciated that the location of communication region 104 disposed on or within card 100 may vary depending on card configuration. For additional information regarding non-contact techniques, see, for example, contactless card standards ISO/IEC 10536 and ISO/IEC 14443, which are hereby incorporated by reference.

[0046] Smartcard body 102 may be manufactured from a sufficiently rigid material, which is resistant to various environmental factors (e.g., physical deterioration, thermal extremes, and ESD (electrostatic discharge)). Materials suitable in the context of the present invention include, for example, PVC (polyvinyl chloride), ABS (acrylonitrile-butadiene-styrol), PET (polyethylene terephthalate), or the like. In a preferred embodiment, chip card 100 conforms to the mechanical requirements set forth in ISO 7810, 7813, and 7816. Body 102 may comprise a variety of shapes, for example, the rectangular ID-1, ID-00, or ID-000 dimensions set forth in ISO-7810. In a preferred embodiment, body 102 is roughly the size and shape of a common credit card and substantially conforms to the ID-1 specification.

[0047] Referring now to Figure 2, IC 110 preferably comprises regions for Random Access Memory (RAM) 216, Read-Only Memory (ROM) 214, Central Processing Unit (CPU) 202, Data Bus (BUS) 210, Input/Output (I/O) 208, and Electrically-Erasable and Programmable Read Only Memory (EEPROM) 212.

[0048] RAM 216 comprises volatile memory, which is used by the card primarily for scratch memory (e.g., to store intermediate calculation results and data encryption processes). RAM 216 preferably comprises at least 256 bytes.

[0049] EEPROM 212 provides a non-volatile memory region which is erasable and rewritable electrically, and which is used to store, inter alia, user data, system data, and application files. In the context of the present invention, EEPROM 212 is suitably used to store a plurality of files related to cardholder information and/or preferences (discussed in greater detail below in conjunction with Figures 3-5). EEPROM 212 preferably comprises at least 8K bytes.

[0050] In a preferred embodiment, CPU 202 implements the instruction set stored in ROM 202, handles memory management (i.e., RAM 216 and EEPROM 212), and coordinates input/output activities (i.e., I/O 208).

[0051] ROM 214 preferably contains, or is "masked" with, the smartcard operating system (SCOS). That is, the SCOS is preferably implemented as hard-wired logic in ROM 214 using standard mask design and semiconductor processing methods well known in the art (e.g., photolithography, diffusion, oxidation, ion implantation, etc.). Accordingly, ROM 214 cannot generally be altered after fabrication. The purpose of such an implementation is to take advantage of the fast access times provided by masked ROMs. ROM 214 suitably comprises about 4K-20K bytes of memory, preferably at least 16K bytes. In this regard, it will be appreciated that alternate memory devices may be used in place of ROM 214. Indeed, as semiconductor technology progresses, it may be advantageous to employ more compact forms of memory, for example, flash-

EEPROMs.

[0052] The SCOS controls information flow to and from the card, and more particularly facilitates storage and retrieval of data stored within EEPROM 212. As with any operating system, the SCOS operates according to a well-defined command set. In this regard, a variety of known smartcard operating systems are suitable for the purpose of this invention, for example, IBM's Multi-Function Card (MFC) Operating System 3.51, the specification of which is hereby incorporated by reference. While the IBM MFC operating system employs the standard tree structure of files and directories substantially in accordance with ISO7816-4 (as detailed below), it will be appreciated by those skilled in the art that other operating system models would be equally suitable for implementation of the present invention. Moreover, it may be advantageous to allow certain aspects of operating system functionality to exist outside the card (i.e., in the form of blocks of executable code) which can be downloaded and executed by the smartcard during a transaction (for example, Java applets, ActiveX objects, and the like).

[0053] Given the general characteristics of smartcard 100 as outlined above, it will be apparent that a wide range of microcontrollers and contact-based smartcard products known in the art may be used to implement various embodiments of the present invention. Suitable smartcards include, for example, the model ST16SF48 card, manufactured by SGS-Thomson Microelectronics, which incorporates a Motorola 6805 microcontroller with 16K ROM, 8K EEPROM, and 384 bytes of RAM. It will be appreciated, however, that particular embodiments of the present invention might require more advanced microcontrollers with greater EEPROM capacity (i.e., in the range of about 12-16K). Such systems are well known in the art.

[0054] Having thus described an exemplary smartcard 100 and IC 110, an overview of a smartcard file structure in accordance with the present invention will now be described with respect to Figures 3-6. Referring now to Figure 3, file structure 400 is preferably used to store information related to cardholder preferences and various data useful for securing transaction settlement and the like. More particularly, file structure 400 preferably comprises cardholder ID application 406, payment system application 408, transaction completion rules application 410, card risk management application 412, optional data objects application 414, and cardholder verification data 404. It will be appreciated by those skilled in the art that the term "application" in this context refers to self-contained regions of data all directed at a particular function (e.g., debit, credit card, automated teller, authentication, authorization etc.) rather than a block of executable software code, although the use of executable modules as part of any particular application falls within the scope of the present invention.

[0055] Cardholder verification data 404 preferably houses data useful in verifying cardholder identity during a transaction. In a preferred embodiment, cardholder verification data 404 comprises two eight-byte cardholder verification numbers (i.e., PIN numbers) referred to as CHV1 and CHV2.

[0056] Cardholder ID application 406 suitably comprises various files related to personal information of the cardholder (e.g., name, addresses, payment cards, driver's license, personal preferences and the like.

[0057] Payment system application 408 suitably comprises information useful in effecting commercial transactions (e.g., account number and expiration date information traditionally stored on a magnetic-stripe credit card). Alternatively, payment system application 408 comprises a full

EMV-compliant application suitable for a wide range of financial transactions.

[0058] Transaction completion rules application 410 suitably comprises data helpful in determining if the conditions for completing a transaction have been met. Transaction completion rules application 410 may ordinarily contain information relevant to whether a requested service is permitted using the smartcard 100.

[0059] Card risk management application 412 suitably comprises information useful for validating that a transaction should be authorized, and for determining the authorization method. The card risk management application 412 may contain data objects relevant to the internal card usage velocity, issuer application data cryptographic data or the like.

[0060] Smartcard 100 may include various optional applications 414 and suitably comprises data useful in expediting the a transaction, including, for example, user preferences, application currency code, application version number, lower consecutive offline limits, upper consecutive offline limits, and the like.

[0061] In each of the above-mentioned applications, sophisticated access and encryption schemes are preferably utilized in order to allow multiple parties to make use of certain file structures while preventing unauthorized entry into others. More specifically, merchants (e.g., various distinct merchants) may create their own tailor-made file structures (i.e., "partner file structures") within card 100. Details of the various security measures employed are described in further detail below in conjunction with Table 40.

[0062] Referring now to Figure 8, smartcard 100 is suitably used in the context of a distributed transaction system. Briefly, cardholders may employ smartcard 100 at various access points 15 which are connected via network 19 to an issuer 10 and at least one merchant 12. Merchant server 12 and issuer 10 suitably comprise various hardware and software components suitable for client host communications as well as a merchant database system 13 and issuer database system 11. In this context, the term "issuer" refers to the organization that actually issues the smartcard and retains some high-level access to certain areas of file structure 400 (detailed below).

[0063] Merchants 12(a), 12(b), and so on, may comprise the various district merchant systems configured to receive data from a smartcard 100 for transaction completion. Each merchant 12 suitably comprises a database 13 and appropriate hardware and software components necessary for completing a transaction over network 19. Network 19 may comprise one or more communication modes, (e.g., the public switched telephone network (PSTN), the Internet, digital and analog wireless networks, and the like).

[0064] Each access point 15 suitably comprises an appropriate card reader for interfacing with smartcard 100 as well as hardware and software suitable for interfacing with a cardholder and performing a transaction over network 19. Access points 15 are preferably located in areas providing convenient access to a cardholder for transaction initiation and completion. Such access points 15 may be located, for example, in airline ticketing and gate areas, rental car facilities, hotel lobbies, travel agencies, and stand-alone kiosks in malls. Furthermore, an individual cardholder might configure his or her personal computer to act as an access point using appropriate software and peripheral hardware.

[0065] In a preferred embodiment of the present invention, data files and directories are stored in a "tree" structure as is known in the art. That is, the smartcard file structure resembles the well-known MS-DOS (Microsoft Disk Operating System) file structure wherein files are logically organized within a hierarchy of directories. Specifically, three types of files are defined in ISO 7816-4: dedicated files (DF), elementary files (EF), and a master file (MF). The master file is analogous to the MS-DOS "root" directory, and contains all other files and directories. Dedicated files are actually directories or "folders" for holding other DFs or EFs. Thus, MF 302 may contain an arbitrary number of DFs 306, and these DFs (e.g., DF 306(a)) may or may not contain other DFs (e.g., DF 308). Elementary files are used to store user data, and may exist within a dedicated file (e.g., EF 310 within DF 306(a)), or within the master file (e.g., EF 304 within MF 302). Higher level DFs (i.e., DFs which house particular applications) are often referred to as application dedicated files (ADFs).

[0066] The MF and each of the DFs and EFs are assigned a unique two-byte file identifier (FID). By convention, the MF is traditionally assigned an FID of "3F00" hex. Selection of an EF or DF by the operating system may then be performed by tracing its entire path starting at the MF. Thus, if the MF contains a DF with a FID "A100", and this DF in turn contains an EF with a FID "A101", then this EF could be referenced absolutely by successive selection of FIDs

3F00, A100, and A101. It will be appreciated that the FID is essentially a file name used by the operating system to select directories and files; it is not intended to indicate a physical address within EEPROM 212. As will be appreciated by those skilled in the art, low-level EEPROM addressing is preferably handled by the SCOS in conjunction with CPU 202.

[0067] Each file preferably has an associated file header containing various indicia of the particular EF, DF, or MF. More particularly, the file header associated with a particular file preferably includes the file identifier (FID), file size, access conditions, and file structure. In this regard, smartcard 100 suitably employs one of four file structures: transparent, linear fixed, linear variable, or cyclic. For the sake completeness, the nature of these file structures will be briefly reviewed.

[0068] A transparent file structure consists of a string of bytes accessed by specifying an offset and byte count. For example, with reference to Table 1 below, given an n-byte string of data, bytes 7 through 10 would be accessed using an offset of six and a length of four.

byte#

1	2	3	4	5	6	7	8	9	10	11	12	13	14	...	...	n
----------------------offset-----------> <---------- length ---------->																

Table 1: Transparent file structure

[0069] A linear fixed file structure comprises a plurality of records of equal length (e.g., a list of phone numbers), wherein access to an individual record is achieved through reference to a record number. In addition, it is possible to refer to the "next" or "previous" record relative to the "current" record (i.e., the most recently accessed record). In contrast, a linear variable file structure comprises records of arbitrary but known length, and is therefore typically more compact than linear fixed data structures.

[0070] A cyclic file structure is a type of linear fixed file wherein a pointer is used to point to the last data set written to. After the last data record is written to, the pointer returns to the first record. That is, a cyclic file comprises a series of records arranged in a "ring." A data structure particularly important with regard to storing records as well as secure messaging in smartcard applications is the BER tag-length-value or "TLV" structure in accordance with ISO/IEC

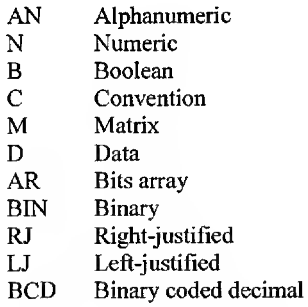
8825, hereby incorporated by reference. In a TLV object, information regarding the type and length of the information is included along with the actual data. Thus, a TLV object comprises a tag, which identifies the type of data (as called out by the appropriate specification), a length field, which indicates the length in bytes of the data to follow, and a value field, which comprises the primary data. For example, the TLV object illustrated in Table 2 below encodes the text "phoenix," which has a length of 7 bytes, and corresponds to a the "city" tag of "8C" hex (a hypothetical tag designation).

Tag	Length	Value						
‘8C’	‘07’	p	H	o	e	n	i	x

Table 2: Exemplary primitive TLV object

[0071] It will be appreciated that the meaning of the various tag values must be known to the system a priori. That is, in order for the tag field to be useful, the smartcard and any external systems communicating with the smartcard must conform to the same tag specification. In this regard, ISO/ IEC 7816-6 defines a series of tags useful in the context of the present invention, as does the IBM MFC 3.2 specification. ISO/IEC 8825 sets forth the basic encoding rules for a TLV system and defines a "template" data object, which can be used as a container for multiple TLV objects. That is, it is often advantageous to encapsulate primitive TLV objects within a larger template, which is itself, a TLV object.

[0072] In the detailed description to follow, various acronyms and abbreviations will be used to refer to particular data types, formats, and the like. A key to these acronyms and abbreviations is presented in Table 3 below.



AN	Alphanumeric
N	Numeric
B	Boolean
C	Convention
M	Matrix
D	Data
AR	Bits array
BIN	Binary
RJ	Right-justified
LJ	Left-justified
BCD	Binary coded decimal

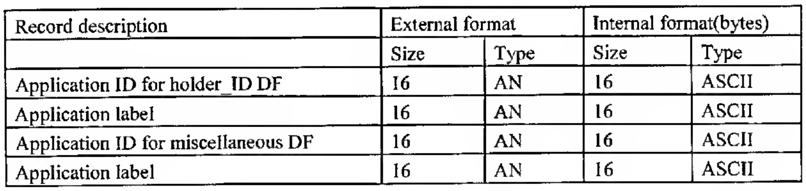
Table 3: Key to acronyms

[0073] In the discussion that follows, the various features of a preferred data structure are in some cases described using particular file structure types (i.e., transparent, fixed, etc.). Those skilled in the art will realize, however, that any of the common smartcard file structure types are typically suitable for implementing any particular data structure. For example, when a file structure is described as including "a plurality of records," it will be understood that such a structure may be designed, for example, using a list of records assembled in a linear fixed file wherein each record is itself a transparent file (and offset values correspond to the various fields). Alternatively, such a structure may be designed using TLV strings assembled in a linear fixed file or within a larger template TLV. This is the case notwithstanding the fact that particular tag values which are for the most part arbitrary are not explicitly listed in the tables that follow.

[0074] Referring now to Figure 4, Cardholder ID application 406 is used to store various information related to the cardholder. More particularly, cardholder ID application 406 preferably comprises directory EF 532, holder_ID DF 502 and miscellaneous DF 530. Holder_ID DF 502 preferably comprises ID EF 504, home EF 506, business EF 508, preferences EF 514, passport EF 516, authentication EF 520, biometric EF 522, and driver EF 518. Miscellaneous EF 530 preferably comprises payment card EF 510, sequence EF 512, issuance EF 511, preferred programs EF

528, and card number EF 526. These files and their respective functions are discussed in detail below.

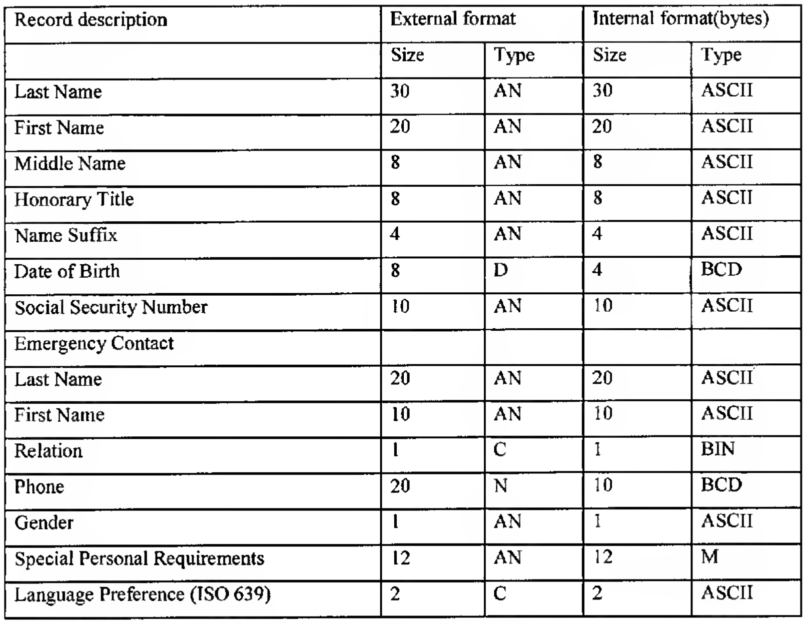
[0075] Directory EF 532 provides a list of application identifiers and labels for the various high-level DF's existing under cardholder ID application 406. That is, this file serves the function of a high-level directory listing which specifies the location (i.e., FID) and application label for each DF in this case, holder_ID DF 502 and miscellaneous DF 530. In a particularly preferred embodiment, directory EF 532 is structured in accordance with EMV 3.0 as shown in Table 4 below. Preferably, each major application (e.g., hotel, airline, etc.) has an associated directory file with a substantially same file structure.



Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
Application ID for holder_ID DF	16	AN	16	ASCII
Application label	16	AN	16	ASCII
Application ID for miscellaneous DF	16	AN	16	ASCII
Application label	16	AN	16	ASCII

Table 4: Exemplary cardholder ID directory EF

[0076] ID EF 504 preferably includes personal information related to the cardholder (e.g., name, date of birth, emergency contact, general preferences, and the like). In a particularly preferred embodiment, member EF 504 comprises the fields set forth in Table 5 below. Italicized field names indicate a subcategory within a particular field.

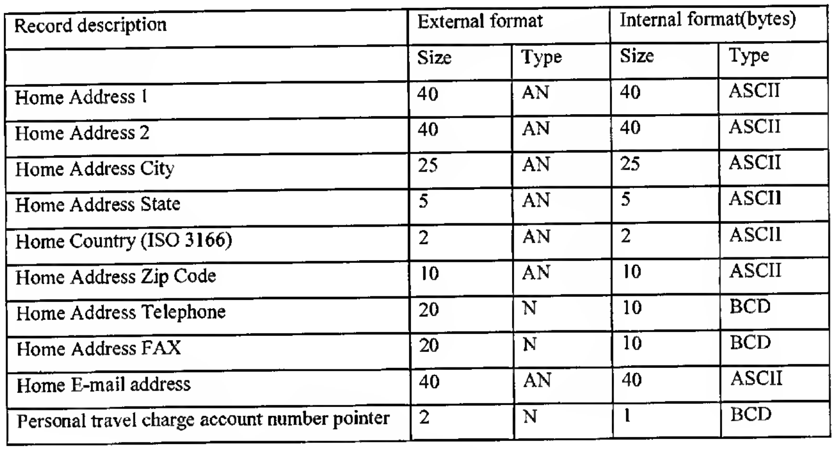


Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
Last Name	30	AN	30	ASCII
First Name	20	AN	20	ASCII
Middle Name	8	AN	8	ASCII
Honorary Title	8	AN	8	ASCII
Name Suffix	4	AN	4	ASCII
Date of Birth	8	D	4	BCD
Social Security Number	10	AN	10	ASCII
Emergency Contact				
Last Name	20	AN	20	ASCII
First Name	10	AN	10	ASCII
Relation	1	C	1	BIN
Phone	20	N	10	BCD
Gender	1	AN	1	ASCII
Special Personal Requirements	12	AN	12	M
Language Preference (ISO 639)	2	C	2	ASCII

Table 5: Exemplary ID EF data structure

[0077] In the above table, and the tables to follow, both internal and external data formats are listed. As the conservation of EEPROM space is of paramount importance, the "internal" format of data (i.e., within EEPROM 212) may be different from the "external" format of the data (i.e., as read by the card reader at an access point 15). Thus, for example, a date field might consist of a four-byte BCD record within the card, but upon reading and processing by the terminal, this data might be converted to an eight-byte decimal value for more convenient processing.

[0078] Home EF 506 preferably includes data related to one or more of the cardholder's home addresses. In a particularly preferred embodiment, home EF 506 comprising the fields set forth in Table 6 below. The personal travel charge account pointer is preferably used to designate a preferred payment card, and consists of a number corresponding to one of the payment card records within payment card EF 510 (detailed below).

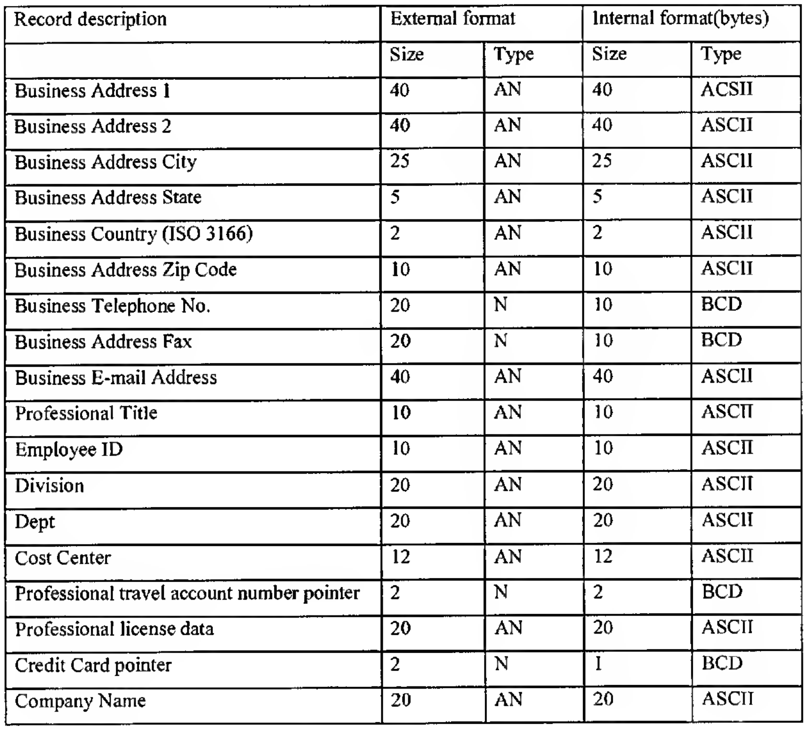


Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
Home Address 1	40	AN	40	ASCII
Home Address 2	40	AN	40	ASCII
Home Address City	25	AN	25	ASCII
Home Address State	5	AN	5	ASCII
Home Country (ISO 3166)	2	AN	2	ASCII
Home Address Zip Code	10	AN	10	ASCII
Home Address Telephone	20	N	10	BCD
Home Address FAX	20	N	10	BCD
Home E-mail address	40	AN	40	ASCII
Personal travel charge account number pointer	2	N	1	BCD

Table 6: Exemplary home EF file structure

[0079] Business EF 508 preferably includes various data related to the cardholder's business (i.e., addresses, phone numbers, and the like). In a particularly preferred embodiment, business EF 508 comprises the fields set forth in

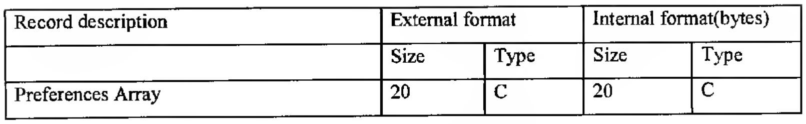
Table 7 below. In this regard, the credit card pointer field is preferably used to point to a payment card record within payment card EF 510 (detailed below). The cost center, dept., division, and employee ID fields are employer-specific, and may or may not apply in a given case.



Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
Business Address 1	40	AN	40	ACSII
Business Address 2	40	AN	40	ASCII
Business Address City	25	AN	25	ASCII
Business Address State	5	AN	5	ASCII
Business Country (ISO 3166)	2	AN	2	ASCII
Business Address Zip Code	10	AN	10	ASCII
Business Telephone No.	20	N	10	BCD
Business Address Fax	20	N	10	BCD
Business E-mail Address	40	AN	40	ASCII
Professional Title	10	AN	10	ASCII
Employee ID	10	AN	10	ASCII
Division	20	AN	20	ASCII
Dept	20	AN	20	ASCII
Cost Center	12	AN	12	ASCII
Professional travel account number pointer	2	N	2	BCD
Professional license data	20	AN	20	ASCII
Credit Card pointer	2	N	1	BCD
Company Name	20	AN	20	ASCII

Table 7: Exemplary business EF file structure

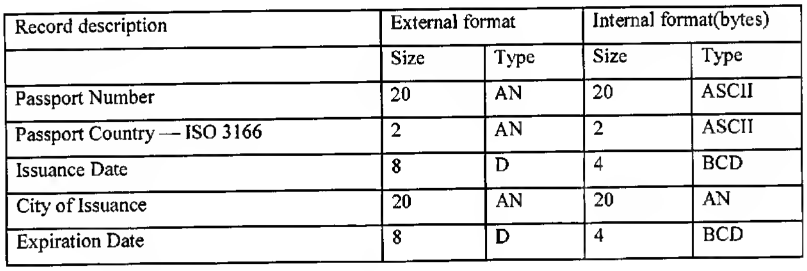
[0080] Preferences EF 514 preferably comprises data related to the cardholder's default personal preferences. In a particularly preferred embodiment, preferences EF 514 include a field comprising an array of preferences as set forth in Table 8 below.



Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
Preferences Array	20	C	20	C

Table 8: Exemplary preferences EF file structure

[0081] Passport EF 516 is preferably used to store cardholder passport information. In a particularly preferred embodiment, passport EF 516 comprises the fields set forth in Table 9 below.



Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
Passport Number	20	AN	20	ASCII
Passport Country — ISO 3166	2	AN	2	ASCII
Issuance Date	8	D	4	BCD
City of Issuance	20	AN	20	AN
Expiration Date	8	D	4	BCD

Table 9: Exemplary passport EF file structure

[0082] Driver EF 516 preferably comprises cardholder driver license data. In a particularly preferred embodiment, driver EF 518 comprises the fields set forth in Table 10 below.

Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
Driver's License No.	20	a	20	ASCII
Driver's License Issuing State/Country	2	a	2	BCD
License Expiration Date	8	D	4	ASCII
License Type	2	C	4	BCD

Table 10: Exemplary driver EF file structure

[0083] Biometric EF 522 is used to store biometric data (preferably encoded) such as fingerprint data, retina scan data, or any other sufficiently unique indicia the card-holder's physical or behavioral characteristics. In a particularly preferred embodiment, biometric EF 522 comprises a single data string as set forth in Table 11 below.

Record description	External format		Internal format (bytes)	
	Size	Type	Size	Type
Biometrics template	100	AN	100	BIN

Table 11: Exemplary biometric EF file structure

[0084] Authentication EF 520 preferably comprises information for static authentication of the cardholder ID 406 application. This data is unique for each card, and is sufficiently complex such that counterfeit values cannot feasibly be created. This prevents creation of "new" counterfeit cards (i.e., cards with new authentication data), but does not prevent creation of multiple copies of the current card.

[0085] In a particularly preferred embodiment, authentication EF 520 includes public key certificate fields as shown in Table 12 below, wherein the external format is identical to the internal format . Preferably, the issuer RSA key is 640 bits long, and the CA key is 768 bits long.

Record description	Internal format(bytes)	
	Size	Type
Signed Static Application Data	80	B
Static Data Authentication Tag List	16	B
Issuer Public Key Certificate	96	B
Issuer Public Key Exponent	1	B
Issuer Public Key Remainder	20	B

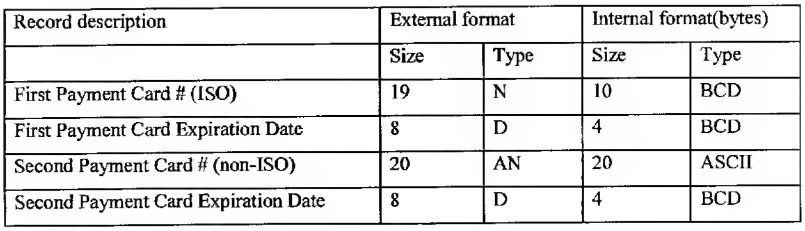
Table 12: Exemplary authentication EF

[0086] Turning now to files under miscellaneous DF 530, preferred programs EF 528 preferably comprise data related to the cardholder's preferences as to airline companies, hotels, and rental car agencies. Specifically, this EF, in a particularly preferred embodiment, may comprise a plurality of records (e.g., three) indicating preferred companies for each type of travel partner as shown in Table 13. The actual data values conform to an arbitrary convention; that is, each airline, hotel, and rental car agency is assigned an arbitrary three-byte code.

Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
Preferred Airlines	9 (3x3)	C	9	C
Preferred Hotels	9	C	9	C
Preferred Rental Cars	9	C	9	C

Table 13: Exemplary programs EF

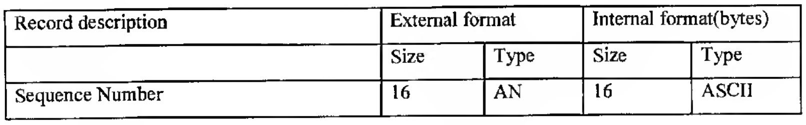
[0087] Payment card EF 510 is preferably used to catalog information related to the cardholder's various payment cards (i.e., debit cards, charge cards, and the like). In a particularly preferred embodiment, payment card EF comprises card numbers and expiration dates for two cards as shown in Table 14. The "ISO" and "non-ISO" designations refer to ISO-7813, which specifies a particular payment card number format. Thus, in a preferred embodiment, either an ISO or non-ISO card number scheme may be used. Moreover, it will be appreciated that this data set is sufficient only for "card not present" transactions, for example, transactions taking place remotely where only the card number and expiration date are required to effect a transaction. Data stored within payment system application 408 (described below) must be used to effect a "card present" transaction.



Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
First Payment Card # (ISO)	19	N	10	BCD
First Payment Card Expiration Date	8	D	4	BCD
Second Payment Card # (non-ISO)	20	AN	20	ASCII
Second Payment Card Expiration Date	8	D	4	BCD

Table 14: Exemplary payment card EF file structure

[0088] Sequence EF 512 preferably includes information used to provide synchronization of the host and smartcard databases. In a particularly preferred embodiment, sequence EF 512 comprises a plurality of records comprising the field set forth in Table 15 below. This number is analogous to a "version" number for the data stored in the application.



Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
Sequence Number	16	AN	16	ASCII

Table 15: Exemplary sequence EF file structure

[0089] Card number EF 526 is used to record a unique number identifying the smartcard, and may also be used for key derivation (as described in further detail below). Preferably, card number EF 526 comprises an eight-byte string as set forth in Table 16 below.

Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
Card Number	8	HEX	8	HEX

Table 16: Exemplary card number EF

[0090] Issuance EF 511 is used to record various details related to the manner in which the application (i.e., cardholder ID DF 406) was created. This file includes information related to the identity of the organization that created the application, as well as information related to the application itself. In a particularly preferred embodiment, issuance EF 511 comprises fields as set forth in Table 17 below.

Field	External format		Internal format (bytes)	
	Size	Type	Size	Type
Country Authority		ISO 3166	2	
Issuer Authority	10	RID - ISO 7816-5	5	HEX
Application version	5	XX.YY	2	BCD
Application expiration date	8	YYYYMM DD	4	BCD
Application effective date	8	YYYYMM DD	4	BCD
Personalizer Code	1	AN	1	ASCII
Personalization Location	1	AN	1	ASCII

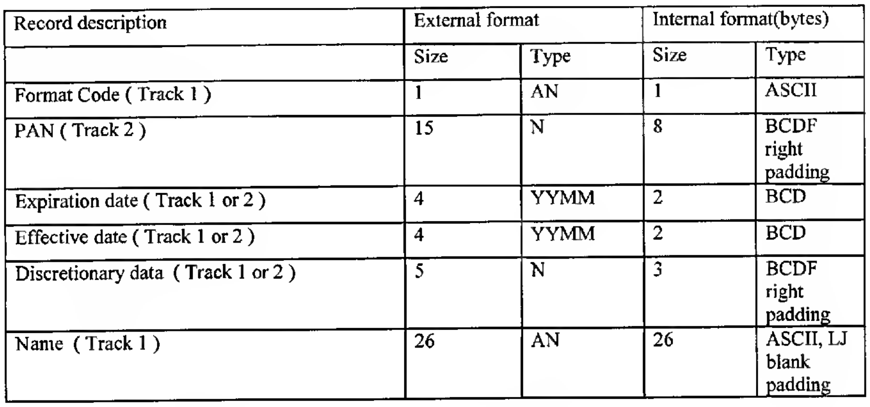
Table 17: Exemplary issuance EF file structure

[0091] The personalizer code field shown in Table 17 refers to the organization that actually "personalizes" the file. That is, before a smartcard may be issued to the cardholder, the database structure must be created within EEPROM 212 (Figure 2), and the initial data values (i.e., default preferences, cardholder name, pin numbers, etc.) must be placed in the appropriate fields within the various EFs. It will be appreciated that, given the nature of the present invention, the smartcard "issuer" and "personalizer" for any given application may not be the same. Therefore, it is advantageous to record various details of the personalization process within smartcard 100 itself. Similar issuance file structures may be provided for the other major applications.

[0092] Referring now to Figure 5, payment system application 408 preferably comprises a directory EF 610, issuer DF 602, and a number of optional DFs 603(a)-(n) for use by partnering financial organizations.

[0093] Directory EF 610 preferably includes a list of application identifiers and labels as described above in the context of cardholder ID application 406.

[0094] Issuer DF 602 comprises pay1 DF 604, which includes data that would traditionally be stored within tracks on a magnetic stripe card (i.e., debit cards, charge cards, and the like). In a preferred exemplary embodiment, pay1 DF 604 comprises a plurality of records having commonly known magnetic-stripe fields as specified in Table 18 below.



Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
Format Code (Track 1)	1	AN	1	ASCII
PAN (Track 2)	15	N	8	BCDF right padding
Expiration date (Track 1 or 2)	4	YYMM	2	BCD
Effective date (Track 1 or 2)	4	YYMM	2	BCD
Discretionary data (Track 1 or 2)	5	N	3	BCDF right padding
Name (Track 1)	26	AN	26	ASCII, LJ blank padding

Table 18: Exemplary Pay1 EF file structure

[0095] Transaction rules application 410 and risk management application 412 may be of similar directory structure (not shown) as is discussed with respect to the cardholder identification application 406, and payment system application 408 discussed above. For example, transaction rules application 410 and risk management directory 412 may contain directories including data relevant to processing restrictions (e.g., application version number, application usage control, effective date check, expiration date check, offline transaction authorization data, issuer authentication data, etc.).

[0096] In the context of smartcard transactions, application 410, 412 may additionally contain directories relevant to data security. Exemplary security directories may include data relevant to: 1) data confidentiality, 2) data integrity, 3) access control, 4) authentication, and 5) non-repudiation. Each of these dimensions is addressed through a variety of security mechanisms. Data confidentiality, which deals with keeping information secret (i.e., unreadable to those without access to a key), is substantially ensured using encryption technology. Data integrity (and data source verification) focuses on ensuring that data remains unchanged during transfer, and typically employs message authentication techniques. Access control involves cardholder verification and other requirements necessary in order for a party to read or update a particular file. Authentication involves ensuring that the card and/or the external device is what it purports to be, and non-repudiation deals with the related task of ensuring that the source of the data or message is authentic (i.e., that a consumer may not repudiate a transaction by claiming that it was "signed" by an unauthorized party).

[0097] Authentication may be preferably performed using a "challenge/response" algorithm. In general, authentication through a challenge/response system involves: 1) generation of a random number by a first party, 2) transmission of the random number to a second party (the "challenge"), 3) encryption of the random number by the second party in accordance with a key known to both parties, 4) transmission of the encrypted random number to the first party (the "response"), 5) encryption of the random number by the first party, and 6) comparison by the first party of the two resulting numbers. In the case where the two numbers match, authentication is successful; if not, the authentication is unsuccessful. Note that authentication can work both ways: the external world might request authentication of a smartcard (internal authentication), and a smartcard might request authentication of the external world (external authentication). A more detailed account of a preferred challenge/response algorithm can be found in the IBM MFC specification.

[0098] In a preferred embodiment, the DES algorithm (Data Encryption Standard) is employed for the various security functions; however, it will be appreciated that any number of other symmetrical or asymmetrical techniques may be used in the context of the present invention. More particularly, there are two general categories of encryption algorithms: symmetric and asymmetric. Symmetric algorithms use the same key for encryption and decryption, for example, DEA (data encryption algorithm) that uses a 56-bit key to encrypt 64-bit blocks of data. Asymmetric algorithms, in contrast, use two different keys: one secret key and one public key. The RSA algorithm, for example, uses two such keys and exploits the computational complexity of factoring very large prime numbers. Additional information regarding these and other cryptographic principles can be found in a number of standard texts, for example: Seberry & Pieprzyk, "Cryptography: An Introduction to Computer Security" (1989); Rhee, "Cryptography and Secure Communications" (1994); Stinson, "Cryptography: Theory and Practice" (1995); "Contemporary Cryptography: The Science of Information Integrity" (1992); and Schneier, "Applied Cryptography" (2d ed. 1996), the contents of which are hereby incorporated by reference.

[0099] Including access conditions within the header of each EF and DF suitably provides access control. This prevents a particular operation (e.g., reading or updating) from being performed on a file unless the required access conditions have been fulfilled. Many different access conditions are appropriate in a smartcard context. For example, the smartcard might require cardholder verification (i.e., request that the cardholder enter a PIN) before a file operation is allowed. Similarly, internal and/or external authentication as described above might be required.

[0100] Figure 7 depicts a flow diagram of an exemplary transaction completion method according to the present invention. An understanding of the method of Figure 7 may be had with reference to Figures 6, 7 and 8. As shown, the method 700 begins with a cardholder presenting the smartcard 100 to initiate transaction completion (step 701). Card 100 is inserted in a card reader 702 provided at an access point 15 and suitable connections are made between communication region 104 on card 100 and the card reader. In a preferred embodiment, physical contacts (contacts 106 in Figure 1) are used, and DATA, CLOCK, RESET, VDD, and GND connections are made. These contacts are electrically activated in a particular sequence, preferably in accordance with ISO 7816-3 (RST to low state, VDD powered, DATA to reception mode, then CLK applied).

[0101] In an alternate embodiment of the transaction device (e.g., smartcard 100), such as the RF transaction device discussed with reference to Figure 9, the communication between the transaction device and the reader may take place in a contactless environment. For example, data may be transmitted between the transaction device and the merchant reader using a RF medium. For a complete description of the method of transferring information between a RF transaction device and a RF reader please refer to U.S. Patent Application No. 10/192,488, filed July 9, 2002, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," incorporated herein by reference.

[0102] Although the present invention is described with reference to a smartcard 100, the invention may be practiced using a RFID transaction device, such as fob 102 of Figure 9. In this case, fob 902 may be placed in communication with a RFID reader 1002 shown in Figure 10. A detailed description of the transfer of data using fob 902, in accordance with the invention, is described below with respect to Figure 10.

[0103] Returning now to the exemplary smartcard processing description discussed above, once the card 100 is presented to the reader 702, the merchant system 704 receives data from the card 100 relative to the applications contained in, for example, the payment system director 408. The card 100 may be configured to direct the merchant system 704 to which card 100 directory or data location from which to retrieve the applications contained thereon. The merchant system 704 receives the application information and compares the information with payment applications data stored on the merchant system 704 (e.g., in merchant database 13) to determines which processing applications are supported by both the card 100 and the merchant system 704 (step 703). The merchant system 704 selects the application with the highest priority, as determined by the hierarchical ordering of the payment applications contained on the card 100 and in the merchant system 704. If no applications are supported, then the transaction may be terminated. For additional information on selecting an application and the response provided by merchant system 704 and card 100, see the ISO 7816-4 specification, incorporated herein by reference.

[0104] Once the appropriate application is selected (step 703), the merchant system 704 then provides the card 100 with a "READ APPLICATION DATA" command (step 705), to retrieve the data objects pertinent to user or issuer authentication (e.g., certification authority public key index, issuer public key certificate, issuer public key exponent, signed static application data, and issuer public key remainder data), and transaction completion (e.g., account or card expiration date, cardholder name, address, issuer identification code, acquirer identification code, etc.). In one exemplary embodiment, the merchant system 704 may store the data received from card 100 in a merchant database 13 for later use.

[0105] The READ APPLICATION DATA command may contain a "GET PROCESSING OPTIONS" command, which prompts the card 100 to present to the reader 702, the appropriate directory or data location to be used during the initiated transaction. In response to the GET PROCESSING OPTIONS command, the card 100 directs the merchant system 704 to the list of supported applications and related data files to be received from the card 100 in step 701 to determine which processing method to perform (e.g., online or offline) for transaction authentication.

[0106] In one exemplary embodiment, the merchant system 704 may provide the card 100 with a "GENERATE AUTHENTICATION CRYPTOGRAM" command ("GENERATE AC" command) discussed below. The GENERATE AC command may not be issued until the transaction has been initiated.

[0107] For offline data authentication (step 707), the merchant system 704 may provide the card 100 a GENERATE AC command, which prompts the merchant system 704 to authenticate the card 100 offline using either static or dynamic data authentication. In general, offline data authentication may be attempted with every transaction. Dynamic data authentication (DDA) data objects stored on the card 100 ordinarily have the highest priority, and if both the merchant system 704 and the card support DDA, then DDA is performed. If the card 100 and the merchant system 704 do not support DDA, but support static data authentication (SDA), then SDA is performed.

[0108] In general, the data relationships used for offline authentication may include a single issuer (or multiple) account issuer EMV Certificate Authority (CA). Where the account is maintained by an issuer, but the card is provided to the user by a third-party merchant (e.g., United Airlines American Express Card, Private Label VISA card, Bank of America MasterCard, etc.), the third-party merchant (sometimes referred to as an "issuing partner") may also have a CA stored on each card 100 which is provided by the issuing partner. Each card 100 may also include an issuing partner Public Key certificate, which may be signed by the issuer EMV CA public key. Additionally, each payment application stored on the card 100 may hold an application DDA Private Key and Public Key Certificate which is signed by the issuer CA Private Key. Thus, for the cryptographic scheme to work, each merchant system 704 need only have access to the issuer CA Public Key scheme, which may be provided to the merchant system 704 by the issuer 10 prior to transaction initiation (step 701).

[0109] During SDA, the card 100 may be in a passive state and the merchant system 704 may be in an active state. That is, the card 100 provides the data to be validated but the merchant system 704 carries out all computations. For example, during SDA fixed signature over data elements held within the card 100 are validated to ensure that the data has not been fraudulently altered since card 100 personalization. The merchant system 704 may use the issuer public key retrieved from the card to decrypt data from the card 100 to obtain a hash. In this way, the merchant system 704 can determine if the hash, obtained through decryption, matches or corresponds to the hash of the actual data objects retrieved from the card 100. If the hashes do not match, then offline SDA fails.

[0110] Alternatively, if the card 100 and the merchant system 704 both support DDA, DDA is performed. DDA is an offline authentication technique in which the card 100 and the merchant system 704 are both active and capable of executing an asymmetric cryptographic algorithm. DDA validates that the card 100 data has not been altered and that the card 100 is genuine. As a part of DDA, the merchant system 704 may validate the card 100 static data as discussed with respect to SDA. In addition, the merchant system 704 requests that the card 100 generate a cryptogram using dynamic data, which is unique to the transaction, and which is retrieved from the card 100 and the merchant 704, and a card DDA Authentication Private Key. The merchant system 704 may decrypt the dynamic signature using the card 100 application DDA Public key recovered from the card data. The merchant system 704 may then compare the decrypted dynamic signature (e.g., hash) to the hash of the original data on the card 100 to see if a match exists. If so, then the merchant system 704 may be assured that the card 100 presented for transaction completion is not counterfeit.

[0111] The results of the offline data authentication process are used to determine if the transaction should be approved offline, online, or if the transaction request should be denied, as is discussed more fully below.

[0112] Should the merchant system 704 determine that the offline authentication can be made and is successful, then the merchant system 704 may examine the data received from the card 100 to see if process restrictions may affect completion of the transaction (step 709). The merchant system 704 may examine, for example, whether the card 100 is expired or if the effective date on the card has been exceeded. The merchant system 704 may also examine whether the application versions contained on the card 100 and the merchant system 704 are compatible, and whether any Application Usage Control Restrictions are in effect. An issuer 10 or cardholder may define various Application Usage Control Restrictions to place limits on for example, card 100 usage, or products or services to be purchased, etc.

[0113] If no processing restrictions exist which prevent transaction completion, the merchant system 704 may seek to verify the cardholder's identity (step 711). The merchant system 704 may use any technique for verifying the cardholder's identity as is found in the art. For example, the merchant system 704 may verify the user information received from the card 100 by, for example, placing the cryptographic information in an algorithm for comparison with known quantities. In another exemplary embodiment, the merchant system 704 may require the cardholder to supply additional secondary identifying indicia (e.g., biometric data or personal security code, or personal identification number), which may be compared against data received from the card 100.

[0114] Once the cardholder's identity is verified (step 711), the merchant system 704 may perform a risk management process (step 713) to determine if certain risk factors exist, which prevent transaction completion. For example, the merchant system 704 may check whether the transaction is over the merchant floor limit, the account number is on an optional merchant exception file, the limit for consecutive offline transactions has been exceeded, the card 100 is a newly-issued card, or the merchant system 704 has forced the transaction online.

[0115] Occasionally, a merchant system 704 may randomly select a transaction for online processing. The merchant system 704 may compile the results of the online processing and store the compiled results in merchant database 13 for later reference.

[0116] As a part of the merchant risk management process (step 713), the merchant system 704 receives data corresponding to the number of times an application transaction has been used (Application Transaction Counter Data). The merchant system 704 stores the Application Transaction Counter Data (ATCD) in merchant database 13 for later use. For example, the merchant system 704 uses the ATCD to guard the transaction against fraud.

[0117] The merchant system 704 may then perform a 1st merchant action analysis to determine if the transaction should be approved offline, sent online for approval, or declined offline (step 715). The merchant system 704 uses the results of the offline data authentication, processing restrictions, merchant risk management data, and rules set in the card 100 and the merchant system 704 in its determination. After determining the disposition of the transaction, the merchant system 704 requests an application cryptogram from the card 100. The type of cryptogram application requested by the merchant system 704 depends on the disposition of the transaction. If the merchant system 704 determines that the transaction should be approved offline, the merchant system 704 may request a Transaction Certificate (TC) application for use in securing transaction approval. If, the merchant system 704 determines that the transaction should proceed online for approval, then the merchant system 704 may request an Authorization Request Cryptogram (ARQC) for a request for approval online. Lastly, if the merchant system 704 determines that the transaction should be declined, the merchant system may request a Application Authentication Cryptogram (AAC) for declining the transaction.

[0118] Online authorization of the transaction may only occur if the merchant system 704 has online capabilities (i.e., establish a direct link with issuer for authorization) (step 719). If the merchant system 704 has online capabilities, the merchant system 704 manipulates and analyzes the offline processing results to determine whether to go on line for online authorization. The results of the analysis may prompt the merchant system 704, to not select "offline decline" or "go online", but instead to select "approve offline", in which case, the merchant system 704 may request a TC from the card 100 and request that the card 100 permit offline approval.

[0119] On the other hand, if the merchant system 704 does not have online capabilities, then the merchant system 704 may retrieve offline processing results from both the merchant system 704 and the card 100 for comparison. The merchant system 704 may compare the results to determine whether to request the card 100 to decline or approve the transaction.

[0120] Upon receiving the 1st application cryptogram request from the merchant system 704 (step 701), the card 100 may perform a 1st Card Action Analysis (step 717). As a sub process thereof, the card 100 may perform a 1st Card Risk Management process to determine the response to be given to the merchant system 704 request for cryptogram. After completion of the 1st Card Action Analysis (step 717) the card may generate an appropriate Application Cryptogram using application data and a secret DES Key (the AC DEA keys) stored on the card 100, and may return the Application Cryptogram to the merchant system 704.

[0121] As noted, the card 100 may return a cryptogram to the merchant system 704 in response to the merchant system's 704 request for a 1st application cryptogram. That is, the card 100 may determine if the transaction should be approved offline, sent to online approval, or should be declined offline. For offline-approved transactions, the card 100 may provide the merchant system with a TC. The card 100 may transmit the TC and the data used to generate it to the merchant system 704. The information transmitted to the merchant system 704 may be used at a later date as evidence that a transaction took place, settle cardholder disputes, or for chargebacks, and the like. The TC may be used by the issuer system 10 to prove that the transaction has not been altered by the merchant attendant to the transaction or the acquirer.

[0122] If the card 100 determines that a transaction should be approved offline, the merchant system does not request a 2nd Merchant Action Analysis from the card 100 (step 725). Instead, the merchant system 704 may move the transaction toward transaction completion (step 733), where the transaction is completed under business as usual standards.

[0123] If the card 100 determines that the transaction should be declined offline, the card 100 may generate a AAC and return the AAC to the merchant system 704. The card 100 may transmit the AAC and the data used to generate it to the merchant system 704, where the data may be used for future cardholder disputes, chargeback purposes, and the like.

[0124] Where the card 100 determines that the transaction should be completed or authorized online, the card 100 may generate a ARQC cryptogram and may forward the ARQC to the merchant system 704. In this case, the merchant system 704 may move directly to online processing (step 721). If the merchant system 704 is unable to go online (step 725), the merchant system 704 may perform a 2nd Card Action Analysis (step 727).

[0125] As noted, the merchant system 704 performs a 1st Merchant Action Analysis to determine if the transaction should be subjected to online authorization. Similarly, card 100 performs a 1st card action analysis to determine if the transaction should be subjected to online authorization. If either the card 100 or the merchant system 704 determines that the transaction requires online authorization, the merchant system 704 transmits the online authorization message to the issuer 10 if the merchant has online capability (step 721). The message includes the cryptogram (e.g., ARQC) generated by the card 100, the data used to generate the cryptogram and the indicators showing offline processing results. In markets that support the ISO 8583 field 55 or equivalent standard, the cryptogram and associated data are compressed into the space available with Track 1 and/or Track 2 data format.

[0126] During online processing, the issuer 10 validates the cryptogram to authenticate the card 100 (step 723). The issuer system 10 may then provide an authorization response to the merchant system 704. The authorization response may include an issuer-generated Authorization Response Cryptogram (ARPC) (derived from the cryptogram generated by the card 100, the authorization response code, card 100 secret DES key (AC DEA Keys)). If the authorization response message transmitted back to the merchant system 704 contains a response cryptogram (ARPC), the card 100 performs issuer authentication by validating that the cryptogram came from a genuine issuer (or its agent). This prevents villainous third parties from circumventing the card 100 security features by simulating online processing and fraudulently approving a transaction to reset counters and indicators.

[0127] The merchant system 704 may receive the issuer authentication data, and if the authentication was successful (i.e., the merchant system 704 received a response cryptogram from the issuer system 10), the merchant system 704 may request a 2nd application cryptogram from the card 100 using the response cryptogram from the issuer system 10 (step 727).

[0128] In some cases, however, especially in a contactless transaction, the cardholder may have removed the card 100 from the field of the reader 702 before transaction completion. If so, the merchant system 704 may alternatively conclude the transaction based on the response it received from the issuer system 10 without any further interaction from the card 100.

[0129] If the merchant system receives no response from the issuer system 10, then the issuer is not authenticated (e.g., the merchant system 704 does not receive a response cryptogram from the issuer system 10), the merchant system 704 may use the response it receives from online processing (if any is received) to decide the outcome of the transaction, in which case, the merchant system 704 may conclude the transaction without any additional interaction with the card 100.

[0130] If the merchant system 704 is unable to go online or the merchant receives a response cryptogram (e.g., issuer 10 authenticated) from the issuer system 10, the merchant system 704 may decide whether to request offline approval or offline decline from card 100. The nature of the request by the merchant system 704 may be dependent upon Merchant Action Codes stored on the merchant system 704 and the Issuer Action Codes stored on the card 100. The Action Codes are guidelines or rules established by the merchant system 704 or issuer 10 which detail the conditions under which a transaction should be approved offline based on the information received during the prior processing steps.

[0131] If the cardholder has not removed card 100 from the field of the reader 702 during processing, the merchant system 704 may provide the card 100 with a 2nd generate AC command, wherein the card 100 may generate a 2nd Application Cryptogram, and the card 100 may set or reset security related parameters. The card 100 may decline an issuer approved transaction based upon the issuer authentication results (step 723) and the Issuer Action Codes stored on the card 100. Alternatively, the card 100 may generate a TC for approved transactions, and an AAC for declined transactions.

[0132] The merchant system 704 may then be forwarded for transaction completion (step 733) under business a usual standard.

[0133] At the end of a smartcard session, contacts 106 are deactivated. Deactivation of contacts 106 is preferably performed in the order specified in ISO 7816-3 (i.e., RST to low state, CLK to low state, DATA to low state, VDD to inactive state). As mentioned above, the VPP contact is not utilized in a preferred embodiment.

[0134] Alternatively, as described in Figure 6, where the card 100 was placed in contactless communication with the merchant system 704 (e.g., reader 702), the card 100 will be deactivated once it is removed from the interrogation field of the reader 702.

[0135] In the context of the present invention, the merchant system 704 ordinarily performs transaction completion (step 733). If the merchant system 704 transmits a clearing message subsequent to an authorization message, the TC (or ARQC in the case of an online issuer not authenticated transaction) is transmitted in the clearing message as well. Or, the merchant system 704 may decline to complete the transaction where the aforementioned analysis of the Action Codes requires it.

[0136] Once the transaction is complete, the merchant system 704 may forward record of the transaction to the appropriate issuer system 10 or acquirer (not shown) for settlement under the merchant system 704 business as usual practice.

[0137] It should be noted that the method 700 may be used in both EMV and non-EMV markets. In both the EMV and non-EMV markets the architecture of the system does not significantly change between the merchant system 704, to the settlement database 706, to the authorization database 708, or to the issuer database 710. In EMV markets, standard EMV messages and responses may be used with contactless cards behaving as EMV compliant tokens although not using the full functionality defined in EMV. In non-EMV markets, standard ISO 8583 messages used in magnetic stripe transaction will be used to transmit information relating to the contactless transactions that shall be packed into the magnetic stripe data.

[0138] Referencing Figures 9-12, in general, the operation of the present invention using a RFID device (e.g., fob 902) may begin when fob 902 is presented for payment, and is interrogated by RFID reader 1004. Fob 902 and RFID reader 1004 may then engage in mutual authentication as described with respect to smartcard 100 and merchant system 704, after which the transponder 102 may provide the transponder identification and/or account identifier to the RFID reader 1004, which may further provide the information to, for example, a merchant system 704 POS device not shown.

[0139] The RFID reader 1004 may be configured to communicate using a RFID internal antenna 906. Alternatively, RFID reader 1004 may include an external antenna 1008 for communication with fob 902, where the external antenna may be made remote to the RFID reader 1004 using a suitable cable and/or data link. RFID reader 1004 may be further in communication with a merchant system POS via a data link (not shown).

[0140] Although the point-of-interaction device is described herein with respect to a merchant point-of-sale (POS) device, the invention is not to be so limited. Indeed, a merchant POS device is used herein by way of example, and the point-of-interaction device may be any device capable of receiving fob account data. In this regard, the POS may be any point-of-interaction device enabling the user to complete a transaction using a fob 902. The POS device may receive the fob 902 information and provide the information to host system for processing.

[0141] A variety of conventional communications media and protocols may be used for data links. For example, the data links referenced herein may be an Internet Service Provider (ISP) configured to facilitate communications over a local loop as is typically used in connection with standard modem communication, cable modem, dish networks, ISDN, Digital Subscriber Lines (DSL), or any wireless communication media. In addition, the merchant system 704, including the POS device and host network, may reside on a local area network which interfaces to a remote network (not shown) for remote authorization of an intended transaction. The merchant system 704 may communicate with the remote network via a leased line, such as a T1, D3 line, or the like. Such communications lines are described in a variety of texts, such as, "Understanding Data Communications," by Gilbert Held, which is incorporated herein by reference.

[0142] Figure 10 illustrates an exemplary block diagram of a RFID reader 1004 in accordance with an exemplary embodiment of the present invention. RFID reader 1004 includes, for example, an antenna 1002 coupled to a RF module 1302, which is further coupled to a control module 1304. In addition, RFID reader 1004 may include an antenna 1008 positioned remotely from the RFID reader 1004 and coupled to RFID reader 1004 via a suitable cable or other wire or wireless connection.

[0143] RF module 1302 and antenna 1002 may be suitably configured to facilitate communication with fob 902. Where fob 902 is formatted to receive a signal at a particular RF frequency, RF module 1302 may be configured to provide an interrogation signal at that same frequency. For example, in one exemplary embodiment, fob 902 may be configured to respond to an interrogation signal of about 13.56 MHz. In this case, RFID antenna 1002 may be 13 MHz and may be configured to transmit an interrogation signal of about 13.56 MHz. That is, fob 902 may be configured to include a first and second RF module (e.g., transponder) where the first module may operate using a 134 kHz frequency and the second RF module may operate using a 13.56 MHz frequency. The RFID reader 1004 may include two receivers which may operate using the 134 kHz frequency, the 13.56 MHz frequency or both. When the reader 1004 is operating at 134 kHz frequency, only operation with the 134 kHz module on the fob 902 may be possible. When the reader 1004 is operating at the 13.56 MHz frequency, only operation with the 13.56 MHz module on the fob 902 may be possible. Where the reader 1004 supports both a 134 kHz frequency and a 13.56 MHz RF module, the fob 902 may receive both signals from the reader 1004. In this case, the fob 902 may be configured to prioritize selection of the one or the other frequency and reject the remaining frequency. Alternatively, the reader 1004 may receive signals at both frequencies from the fob upon interrogation. In this case, the reader 1004 may be configured to prioritize selection of one or the other frequency and reject the remaining frequency.

[0144] Further, protocol/sequence controller 1314 may include an optional feedback function for notifying the user of the status of a particular transaction. For example, the optional feedback may be in the form of an LED, LED screen and/or other visual display which is configured to light up or display a static, scrolling, flashing and/or other message and/or signal to inform the fob 902 user that the transaction is initiated (e.g., fob is being interrogated), the fob is valid (e.g., fob is authenticated), transaction is being processed, (e.g., fob account number is being read by RFID reader) and/or the transaction is accepted or denied (e.g., transaction approved or disapproved). Such an optional feedback may or may not be accompanied by an audible indicator (or may present the audible indicator singly) for informing the fob 902 user of the transaction status. The audible feedback may be a simple tone, multiple tones, musical indicator, and/or voice indicator configured to signify when the fob 902 is being interrogated, the transaction status, or the like.

[0145] RFID antenna 1002 may be in communication with a transponder 1006 for transmitting an interrogation signal and receiving at least one of an authentication request signal and/or an account data from fob 902. Transponder 1006 may be of similar description as transponder 914 of Figure 9. In particular, transponder 1006 may be configured to send and/or receive RF signals in a format compatible with antenna 1002 in similar manner as was described with respect to fob transponder 914. For example, where transponder 1006 is 13.56 MHz RF rated antenna 1002 may be 13.56 MHz compatible. Similarly, where transponder 1006 is ISO/IEC 14443 rated, antenna 1002 may be ISO/IEC 14443 compatible.

[0146] RF module 1302 may include, for example, transponder 1006 in communication with authentication circuitry 1008 which may be in communication with a secure database 1010. Authentication circuitry 1008 and database 1010 may be of similar description and operation as described with respect to authentication circuitry 910 and secure memory database 912 of Figure 9. For example, database 1010 may store data corresponding to the fob 902 which are authorized to transact business over system 100. Database 1010 may additionally store RFID reader 1004 identifying information for providing to fob 902 for use in authenticating whether RFID reader 1004 is authorized to be provided the fob account number stored on fob database 914.

[0147] Authentication circuitry 1008 may be of similar description and operation as authentication circuitry 910. That is, authentication circuitry 1008 may be configured to authenticate the signal provided by fob 902 in similar manner as is discussed with reference to the merchant system 704 and smartcard 100. As is described more fully below, fob 902 and RFID reader 1004 may engage in mutual authentication. In this context, "mutual authentication" may mean that operation of the system 100 may not take place until fob 902 authenticates the signal from RFID reader 1004, and RFID reader 1004 authenticates the signal from fob 902.

[0148] Authentication circuitry 1008 may additionally be in communication with a protocol/sequence controller 1314 of similar operation and description as protocol/sequence controller 908 of Figure 9. That is, protocol/sequence device controller 1314 may be configured to determine the order of operation of the RFID reader 1004 components. For example, Figure 11 illustrates an exemplary decision process under which protocol/sequence controller 1314 may operate. Protocol/sequence controller 1314 may command the different components of RFID reader 1004 based on whether a fob 902 is present (step 502). For example, if a fob 902 is not present, then protocol/sequence controller 1314 may command the RFID reader 1004 to provide an uninterrupted interrogation signal (step 504). That is, the protocol/sequence controller 1314 may command the authentication circuit 1008 to provide an uninterrupted interrogation signal until the presence of a fob 902 is realized. If a fob 902 is present, the protocol/sequence controller 1314 may command the RFID reader 1004 to authenticate the fob 902 (step 506).

[0149] As noted above, authentication may mean that the protocol/sequence controller 1314 may command the authentication circuit 1008 to provide fob 902 with an authorization code. If a response is received from fob 902, protocol/sequence controller may determine if the response is a response to the RFID reader 1004 provided authentication code, or if the response is a signal requiring authentication (step 508). If the signal requires authentication, then the protocol/sequence controller 1314 may activate the authentication circuit as described above (step 506). On the other hand, if the fob 902 signal is a response to the provided authentication code, then the protocol/sequence controller 1314 may command the RFID reader 1004 to retrieve the appropriate security key for enabling recognition of the signal (step 510). That is, the protocol/sequence controller 1314 may command the authentication circuit 1008 to retrieve from database 1010 a security key (e.g., transponder system decryption key), unlock the signal, and compare the signal to the signal provided by the RFID reader 1004 in the authentication process (e.g., step 506). If the signal is recognized, the protocol/sequence controller 1314 may determine that the fob 902 is authorized to access the transaction system (step 512). If the signal is not recognized, then the fob 902 is considered not authorized, in which case, the protocol/sequence controller 1314 may command the RFID controller to interrogate for authorized fobs (step 504).

[0150] Once the protocol/sequence controller 1314 determines that the fob 902 is authorized, the protocol/sequence controller 1314 may seek to determine if additional signals are being sent by fob 902 (step 514). If no additional signal is provided by fob 902, then the protocol/sequence controller 1314 may provide all the components of RFID reader 1004 to remain idle until such time as a signal is provided (step 516). Contrarily, where an additional fob 902 signal is provided, the protocol/sequence controller 1314 may determine if the fob 902 is requesting access to the merchant point-of-sale terminal (e.g., POS device) or if the fob 902 is attempting to interrogate the RFID reader 1004 for return (e.g., mutual) authorization (step 518). Where the fob 902 is requesting access to a merchant POS device, the protocol/sequence controller 1314 may command the RFID reader 1004 to open communications with the POS device (step 524).

[0151] On the other hand, if the protocol/sequence controller 1314 determines that the fob 902 signal is a mutual interrogation signal, then the protocol/sequence controller 1314 may command the RFID reader 1004 to encrypt the signal (step 520). The protocol/sequence controller 1314 may command the encryption authentication circuit 1018 to retrieve from database 1020 the appropriate encryption key in response to the fob 902 mutual interrogation signal. The protocol/sequence controller 1314 may then command the RFID reader 1004 to provide the encrypted mutual interrogation signal to the fob 902 (step 522). The protocol/sequence controller 1314 may command the authentication circuit 1018 to provide an encrypted mutual interrogation signal for the fob 902 to mutually authenticate. Fob 902 may then receive the encrypted mutual interrogation signal and retrieve from authentication circuitry 1018 a RFID reader 1004 decryption key.

[0152] Although an exemplary decision process of protocol/sequence controller 1314 is described, it should be understood that a similar decision process may be undertaken by protocol/sequence controller 908 in controlling the components of fob 902. Indeed, as described above, protocol/sequence controller 1314 may have similar operation and design as protocol/sequence controller 908.

[0153] Encryption/decryption component 1018 may be further in communication with a secure account number database 1020 which stores the security keys necessary for decrypting the encrypted fob account number. Upon appropriate request from protocol/sequence controller 1314, encryption/decryption component (e.g., circuitry 1018) may retrieve the appropriate security key, decrypt the fob account number and forward the decrypted account number to protocol sequence controller 1314 in any format readable by any later connected POS device. In one exemplary embodiment, the account number may be forwarded in a conventional magnetic stripe format compatible with the ISO/IEC 7813 standard. Upon receiving the account number in magnetic stripe format, protocol/sequence controller 1314 may forward the account number to POS device. POS device may receive the decrypted account number and forward the magnetic stripe formatted account number to a merchant network for processing under the merchant's business as usual standard. In this way, the present invention eliminates the need of a third-party server. Further, where the POS device receives a response from a merchant network (e.g., transaction authorized or denied), protocol/sequence controller 1314 may provide the merchant network response to the RF module 1302 for optically and/or audibly communicating the response to the fob 902 user.

[0154] Figure 12 illustrates an exemplary flow diagram for the operation of an exemplary transaction system according to the present invention utilizing a RFID fob 902 and a RFID reader 1004. The process is initiated when a customer desires to present a fob 902 for payment (step 802). Upon presentation of the fob 902, the merchant initiates the RF payment procedure via a RFID reader 1004 (step 804). In particular, the RFID reader 1004 sends out an interrogation signal to scan for the presence of fob 902 (step 806). The RF signal may be provided via the RFID reader 1004 antenna 1006 or optionally via an external antenna 1008. The customer then may present the fob 902 for payment (step 808) and the fob 902 is activated by the RF interrogation signal provided.

[0155] The fob 902 and the RFID reader 1004 may then engage in mutual authentication (step 810). Where the mutual authentication is unsuccessful, an error message may be provided to the customer via the RFID optical and/or audible indicator (step 814) and the transaction may be aborted (step 816). Where the mutual authentication is successful (step 812), the RFID reader 1004 may provide the customer with an appropriate optical and/or audible message (e.g., "transaction processing" or "wait") (step 818).

[0156] Once the fob 902 and RFID reader 1004 mutually authenticate, the RFID transaction may proceed in accordance with the method described respecting smartcard 100 and Figure 7. Particularly, the RFID reader 1004 may act as a pass through device forwarding information from the fob

902 and the merchant system 704 for authentication and authorization according to steps 701-733. The merchant system 704 and the fob 902 may determine if the transaction should be authorized for offline completion, forwarded to an issuer for online authorization, or declined authorization offline. As such, it should be understood that the fob database 912, 914 may be of similar construction and operation as is discussed with the data storage of smartcard 100. Thus, the fob 902 may be operable to return similar responses to the merchant system 704 as is discussed with reference to the responses of smartcard 100. After the RFID reader 1004 and the fob 902 mutually authenticate, the transaction may proceed to the transaction authentication, user identify verification, and transaction completion process of Figure 7.

[0157] It should be noted that the transaction account associated with the fob 902 may include a restriction, such as, for example, a per purchase spending limit, a time of day use, a day of week use, certain merchant use and/or the like, wherein an additional verification is required when using the fob outside of the restriction. The restrictions may be personally assigned by the fob 902 user, or the account provider. For example, in one exemplary embodiment, the account may be established such that purchases above $X (i.e., the spending limit) must be verified by the customer. Such verification may be provided using a suitable personal identification number (PIN) which may be recognized by the RFID reader 1004 or a payment authorization center (not shown) as being unique to the fob 902 holder (e.g., customer) and the correlative fob 902 transaction account number. Where the requested purchase is above the established per purchase spending limit, the customer may be required to provide, for example, a PIN, biometric sample and/or similar secondary verification to complete the transaction.

[0158] Where a verification PIN is used as secondary verification the verification PIN may be checked for accuracy against a corroborating PIN which correlates to the fob 902 transaction account number. The corroborating PIN may be stored locally (e.g., on the fob 902, or on the RFID reader 1004) or may be stored on a database (not shown) at the payment authorization center. The payment authorization center database may be any database maintained and operated by the fob 902 transaction account provider.

[0159] While the example transactions set forth above are described in general terms, the particular nature of data flow to and from the appropriate memory locations within the card will be apparent to those skilled in the art.

[0160] Moreover, although the inventions set forth herein have been described in conjunction with the appended drawing figures, those skilled in the art will appreciate that the scope of the invention is not so limited. For example, although the preferred embodiment of the invention is discussed in the context of a standard, credit card-sized smartcard with external contacts, it will be appreciated that virtually any portable memory device suitably configured may be utilized to practice this invention, for example, contactless cards, optical cards, minicards, "super-smart" cards, and the like. Hence, various modifications in the design and arrangement of the components and steps discussed herein may be made without departing from the scope of the invention as set forth in the appended claims.